

WE CLAIM:

1. A method of establishing a virtual private network tunnel, the method comprising:

receiving, from a user whose IP address is not known
5 in advance, a first request to form an encrypted tunnel
with a security gateway;

forming the encrypted tunnel;

authenticating the user;

determining an IP address of the user;

10 establishing a correspondence between the IP address
and a first shared secret authorized for the user;

receiving a second request from the user to form a
virtual private network tunnel, the request incorporating
a second shared secret;

15 determining whether the first shared secret matches
the second shared secret; and

forming the virtual private network tunnel when the
first shared secret matches the second shared secret.

2. The method of claim 1, wherein the first request
20 comprises a request to form a Hypertext Transfer Protocol
over Secure Socket Layer session.

3. The method of claim 1, wherein the authenticating
step comprises receiving and verifying a
username/password pair from the user.

25 4. The method of claim 1, wherein the second request
comprises a request to form an IPSec tunnel.

5. The method of claim 1, wherein the establishing step
comprises comparing a username and password provided by
the user with a database of usernames, passwords and
30 shared secrets.

6. The method of claim 1, wherein the second request incorporates a hashing function based on the second shared secret.

7. The method of claim 1, wherein the step of determining whether the first shared secret matches the second shared secret comprises attempting to decrypt at least a portion of the second request.

8. The method of claim 1, wherein the establishing step comprises making an entry in an IPsec table, the entry comprising the IP address and the first shared secret.

9. The method of claim 8, wherein the entry is a temporary entry that is deleted after the occurrence of a predetermined event.

10. The method of claim 9, wherein the predetermined event comprises a passage of a predetermined time.

11. The method of claim 9, further comprising the step of tearing down the virtual private network tunnel when the temporary entry is deleted.

12. A computer program embodied in a machine-readable medium, the computer program comprising instructions for controlling a security gateway to perform the following steps:

receiving, from a user whose IP address is not known in advance, a first request to form an encrypted tunnel with a security gateway;

forming the encrypted tunnel;

authenticating the user;

determining an IP address of the user;

establishing a correspondence between the IP address and a first shared secret authorized for the user;

receiving a second request from the user to form a virtual private network tunnel, the request incorporating a second shared secret;

determining whether the first shared secret matches the second shared secret; and

forming the virtual private network tunnel when the first shared secret matches the second shared secret.

13. The computer program of claim 12, wherein the first request comprises a request to form a Hypertext Transfer Protocol over Secure Socket Layer session.

14. The computer program of claim 12, wherein the authenticating step comprises receiving and verifying a username/password pair from the user.

15. The computer program of claim 12, wherein the second request comprises a request to form an IPsec tunnel.

16. The computer program of claim 12, wherein the establishing step comprises comparing a username and password provided by the user with a database of usernames, passwords and shared secrets.

17. The computer program of claim 12, wherein the second request incorporates a hashing function based on the second shared secret.

18. The computer program of claim 12, wherein the step of determining whether the first shared secret matches the second shared secret comprises attempting to decrypt at least a portion of the second request.

19. A security gateway, comprising:

means for receiving, from a user whose IP address is not known in advance, a first request to form an encrypted tunnel with a security gateway;

means for forming the encrypted tunnel;

means for authenticating the user;
means for determining an IP address of the user;
means for establishing a correspondence between the
IP address and a first shared secret authorized for the
5 user;

means for receiving a second request from the user
to form a virtual private network tunnel, the request
incorporating a second shared secret;

means for determining whether the first shared
10 secret matches the second shared secret; and

means for forming the virtual private network tunnel
when the first shared secret matches the second shared
secret.

20. A security gateway, comprising:

15 a first port configured for communication with the
Internet;

a second port configured for communication with a
private network; and

at least one processor configured to:

20 receive, via the first port, a first request to
form an encrypted tunnel with a security gateway
from a user whose IP address is not known in
advance;

form the encrypted tunnel;

25 authenticate the user;

determine an IP address of the user;

establish a correspondence between the IP
address and a first shared secret authorized for the
user;

30 receive a second request from the user to form
a virtual private network tunnel, the request
incorporating a second shared secret;

determine whether the first shared secret
matches the second shared secret; and

form the virtual private network tunnel when the first shared secret matches the second shared secret.

21. A method of establishing a virtual private network tunnel, the method comprising:

receiving, from a user whose IP address is not known in advance, a first request to form an encrypted tunnel with a security gateway;

forming the encrypted tunnel;

authenticating the user;

determining an IP address of the user;

establishing a correspondence between the IP address and a subject of a digital certificate;

receiving a second request from the user to form a virtual private network tunnel, the request incorporating the digital certificate;

determining that the subject of the digital certificate is an expected subject; and

forming the virtual private network tunnel when the subject of the digital certificate is the expected subject.